PATENT
Attorney Docket No. 0023-0162

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	)	
Ross W. Callon	)	Group Art Unit: 2144
	)	
Serial No.: 10/080,865	)	Examiner: M. Delgado
	)	
Filed: February 21, 2002	)	
	)	
For: DISTRIBUTED FILTERING FOR NETWORKS	)	

APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Window, Mail Stop Appeal Brief – Patents
Randolph Building
401 Dulany Street
Alexandria, Virginia 22314

Sir:

This Appeal Brief is submitted in response to the Final rejection mailed May 23, 2006 and in support of the Notice of Appeal filed September 25, 2006.

I. REAL PARTY IN INTEREST

The real party in interest in this appeal is Juniper Networks, Inc.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals, interferences or judicial proceedings.

III. STATUS OF CLAIMS

Claims 1-6, 9-15, 17-38, 40-43, 45-51, 61, 62 and 64 are pending in this application. Claims 7, 8, 16, 39, 44, 52-60 and 63 were previously canceled without prejudice or disclaimer. Claims 1-6, 9-15, 17-38, 40-43, 45-51, 61, 62 and 64 are the subject of the present appeal.

IV. STATUS OF AMENDMENTS

No Amendment has been filed subsequent to the Final Office Action mailed May 23, 2006. Appellant notes that an After Final Request for Reconsideration was filed on July 24, 2006. An Advisory Action mailed August 23, 2006 indicates that the Request for Reconsideration was not persuasive.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Each of the independent claims involved in this appeal is recited below, followed in parenthesis by examples of where support can be found in the specification and drawings for the claimed subject matter. In addition, each dependent claim argued separately below is also summarized in a similar manner.

Claim 1 recites: A system for detecting and responding to an attack, comprising: a first device attached to a network (Fig. 5, 500, page 12, paragraph 50) and configured to: detect an attack based on received traffic (page 12, paragraph 50), create attack information (page 12, paragraph 50), and forward the attack information to the network using a link state routing protocol or a path vector routing protocol (page 13, paragraph 57; pages 18-19, paragraphs 73-

78); and a second device configured to receive the attack information and detect particular traffic based on the attack information (page 13, paragraph 57).

Claim 2 recites: The system of claim 1, wherein the first device comprises a firewall filter (page 12, paragraph 50).

Claim 4 recites: The system of claim 1, wherein the first device comprises: a packet generating element configured to generate a link state routing packet that includes the attack information (page 13, paragraph 57).

Claim 6 recites: The system of claim 1, wherein the first device forwards the attack information using a path vector routing packet (page 19, paragraph 78).

Claim 14 recites: A method of detecting and responding to an attack, comprising: detecting an attack at a first device based on incoming traffic (Fig. 4, 410; page 10, paragraph 45); generating attack information defining characteristics of the attack (Fig. 4, 420; page 10, paragraph 45; sending the attack information to a second device in a network using at least one of a link state routing packet or a path vector routing packet (Fig. 4, 430; pages 18-19, paragraphs 73-78); and detecting traffic at the second device based on the attack information (page 13, paragraph 57).

Claim 19 recites: The method of claim 14, further including: authenticating the attack information at the second device (page 24, paragraph 0102).

Claim 25 recites: A device for detecting an attack, comprising: an attack detection element configured to detect an attack in incoming traffic (Fig. 5, 570; page 12, paragraph 50); an attack information generator configured to generate attack information defining characteristics of the attack (Fig. 5, 560; page 12, paragraph 50); and a transmitting element configured to transmit the attack information to a device on a network using at least one of a link state routing protocol or a path vector routing protocol (Fig. 5, 530; pages 18-19, paragraphs 73-78).

Claim 33 recites: A method of detecting an attack, comprising: monitoring incoming traffic at a first device to detect an attack (Fig. 4, 410; page 10, paragraph 45); generating attack information defining characteristics of the attack (Fig. 4, 420; page 10, paragraph 45); and transmitting the attack information to a second device via a network using a link state routing protocol, a path vector routing protocol, a markup language protocol or a hypertext protocol (Fig. 4, 430; pages 18-19, paragraphs 73-78).

Claim 40 recites: The method of claim 33, wherein the transmitting includes: sending the attack information using a link state routing protocol (page 13, paragraph 57).

Claim 43 recites: A device for responding to an attack, comprising: a receiver configured to receive attack information from a first device that sent the attack information (Fig. 7, 760;

page 16, paragraph 66); a configuration element configured to configure a second device based on the received attack information (Fig. 7, 770; page 16, paragraph 67); and a transmitting element for transmitting the attack information to another device using a link state routing protocol, a path vector routing protocol, a markup language protocol or a hypertext protocol (Fig. 7, 730; page 17, paragraphs 68 and 70, pages 18-19, paragraphs 73-78).

Claim 61 recites: A method for responding to an attack, comprising: receiving attack information at a central management system from a first device via a network (Fig. 5, 1010; page 25, paragraph 0104); managing a response to the attack at the central management system (page 26, paragraph 0106); receiving, at the central management system, additional attack information from other devices via the network (page 25, paragraph 0104); and communicating, by the central management system, information associated with the additional attack information to the first device (page 26, paragraph 0105).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 61, 62 and 64 have been rejected under 35 U.S.C. § 102(e) as being anticipated by Chen et al. (U.S. Patent Application Publication No. 2002/0032854; hereinafter Chen).

B. Claims 1-6, 9-15, 17, 18, 20-29, 32-38, 40-43, 45-48, 50 and 51 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Goldstone (U.S. Patent Application Publication No. 2002/0101819) in view of Fedyk et al. (U.S. Patent No. 6,560,654; hereinafter Fedyk).

C. Claims 19, 30, 31 and 49 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Goldstone in view of Fedyk and further in view of Nguyen et al. (U.S. Patent Application Publication No. 2002/0016926; hereinafter Nguyen).

VII. ARGUMENT

A. Rejection under 35 U.S.C. § 102 based on Chen

1. Claims 61, 62 and 64

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). A proper rejection under 35 U.S.C. § 102 requires that a single reference teaches every element set forth in the claim, either expressly or inherently. See M.P.E.P. § 2131.

With these principles in mind, claim 61 recites a method for responding to an attack that includes receiving attack information at a central management system from a first device via a network and managing a response to the attack at the central management system. Claim 61 also recites receiving, at the central management system, additional attack information from other devices via the network and communicating, by the central management system, information associated with the additional attack information to the first device.

The Final Office Action states that server 101 of Chen is equivalent to the central management system recited in claim 61 and that attack host 113 of Chen is equivalent to the claimed first device (Final Office Action – page 3). The Final Office Action also states that Chen discloses managing a response to an attack at the central management system and that the central management system receives additional attack information from other devices and points to Fig. 2, elements 106, 107 and 109 along with paragraph 45, lines 1-24 of Chen for support

(Final Office Action – page 3).

Fig. 2 of Chen illustrates an edge router 102 coupled to routers 103-111. Chen at paragraph 45 discloses that edge router 102 creates duplicate programs of itself and forwards these duplicate programs to routers 106, 107, 109 and 110. Routers 106, 107, 109 and 110 then stop traffic from attack hosts 113, 114, 116 and 117 from reaching server 101. Chen at paragraph 45 further discloses that when the attack on server 101 has ended, the mobile packet filtering programs installed on routers 106, 107, 109 and 110 send the history log of the attack to the original mobile packet filtering program installed on edge router 102.

Chen, however, does not disclose or suggest that server 101, alleged to be equivalent to the central management system of claim 61, receives additional attack information from any of devices 106, 107 and 109, which are alleged to be equivalent to the other devices recited in claim 1. In contrast, routers 106, 107 and 109 merely forward attack logs to edge router 102 after the attack has ended. Routers 106, 107 and 109 clearly do not forward additional attack information to server 101, as would be required by claim 61 based on the alleged equivalence of the elements in Chen with the features recited in claim 61.

Claim 61 also recites communicating, by the central management system, information associated with the additional attack information to the first device. The Final Office Action states that Chen discloses this feature and points to paragraph 45, lines 1-24 for support (Final Office Action – page 3). As discussed above, Chen at paragraph 45 discloses that a mobile packet filtering program installed on edge router 102 is moved to routers 106, 107, 109 and 110 and that after an attack has ended, routers 106, 107, 109 and 110 send a history log to edge router 102. This portion of Chen clearly does not disclose or suggest that server 101 receives additional

attack information from routers 106, 107, 109 and 110, much less communicates information associated with the additional attack information to attack host 113, as would be required by claim 61 based on the alleged equivalence of the elements in Chen with the features recited in claim 61.

For at least these reasons, Appellant respectfully submits that the imposed rejection of claim 61 under 35 U.S.C. § 102 based on Chen is improper. Accordingly, reversal of the rejection of claims 61, 62 and 64 is respectfully requested.

B. Rejection under 35 U.S.C. § 103 based on Goldstone in view of Fedyk

As discussed above, the initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention always rests upon the Examiner. In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the Examiner must provide a factual basis to support the conclusion of obviousness. In re Warner, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967). Based upon the objective evidence of record, the Examiner is required to make the factual inquiries mandated by Graham v. John Deere Co., 86 S.Ct. 684, 383 U.S. 1, 148 USPQ 459 (1966). The Examiner is also required to explain how and why one having ordinary skill in the art would have been realistically motivated to modify an applied reference and/or combine applied references to arrive at the claimed invention. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988).

In establishing the requisite motivation, it has been consistently held that the requisite motivation to support the conclusion of obviousness is not an abstract concept, but must stem from the prior art as a whole to impel one having ordinary skill in the art to modify a reference or

to combine references with a reasonable expectation of successfully achieving some particular realistic objective. See, for example, Interconnect Planning Corp. v. Feil, 227 USPQ 543 (Fed. Cir. 1985). Consistent legal precedent admonishes against the indiscriminate combination of prior art references. Carella v. Starlight Archery, 804 F.2d 135, 231 USPQ 644 (Fed. Cir. 1986); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 227 USPQ 657 (Fed. Cir. 1985).

1. Claims 1, 3, 5, 9-15, 17, 20-28 and 32

Claim 1 recites a system for detecting and responding to an attack that includes a first device attached to a network and configured to detect an attack based on received traffic and create attack information. Claim 1 also recites that the first device is configured to forward the attack information to the network using a link state routing protocol or a path vector routing protocol. The Final Office Action admits that Goldstone does not disclose this latter feature, but states that Fedyk discloses a router layer and that the advantage of using the link state routing protocol is to rapidly pass on routing information to other routers in a network and points to col. 1, lines 25-40 of Fedyk for support (Final Office Action – page 4). The Final Office Action further states that it would have been obvious to improve on Goldstone "by using the link state routing protocol method of Fedyk to provide a rapid response to DOS attack and thus reduce the time taken to recover from the attack" (Final Office Action – page 5). Appellant respectfully disagrees.

Fedyk at col. 1, lines 25-40 discloses that link state routing protocols are conventionally used to distribute routing information. Appellant respectfully submits that transmitting attack information using a link state routing protocol or a path vector routing protocol is significantly

different than using a link state routing protocol in the manner it was intended to be used (i.e., to transmit routing information). As discussed in Appellant's specification at paragraph 73, for example, advertising attack information using such a routing protocol enables the attack information to be sent without having to design/use a special purpose flooding mechanism. This greatly simplifies the process for advertising attack information and enables the information to be communicated in an efficient manner. Neither Goldstone nor Fedyk, taken singly or in combination, discloses or suggests using a link state routing protocol or a path vector routing protocol to forward attack information, as required by claim 1.

Therefore, as a factual matter, the combination of Goldstone and Fedyk does not disclose or suggest each of the features of claim 1.

In addition, even if, for the sake of argument, the combination of Goldstone and Fedyk could be fairly construed to disclose or suggest all the features of claim 1, Appellant respectfully submits that the alleged motivation to combine these references does not meet the requirements of 35 U.S.C. § 103.

For example, the Final Office Action states that it would have been obvious to improve on Goldstone's invention "by using the link state routing protocol method of Fedyk in order to provide a rapid response to DOS attack and thus reduce the time taken to recover from the attack" (Final Office Action – page 5). This alleged motivation for combining Fedyk with Goldstone is merely a conclusory statement providing an alleged benefit of the combination. No portion of either reference is pointed to as providing objective motivation for the combination. Such motivation does not satisfy the requirements of 35 U.S.C. § 103.

Appellant further asserts that Goldstone is directed to preventing a denial of service attack in a network (Goldstone – Abstract). Fedyk, in contrast, is directed to managing message traffic in a link state routing network (Fedyk – col. 1, lines 8-11). These two references are unrelated, other than the fact that each of these references may involve network communications. Appellant asserts that one of ordinary skill in the art would not have looked to combine features from these two references due to the disparate nature of these references. That is, the mere fact that both of these references may involve network communications does not mean that it would have been obvious to combine features from these clearly disparate disclosures.

The mere fact that one reference allegedly provides some missing disclosure with respect to a claim does not satisfy the requirements of 35 U.S.C. § 103 as to why it would have been obvious to combine the references. For at least these reasons, Appellant asserts that it would not have been obvious to combine these two references absent impermissible hindsight in an attempt to reconstruct Appellant's invention.

For at least these reasons, Appellant respectfully submits that the rejection of claim 1 under 35 U.S.C. § 103 based on the combination of Goldstone and Fedyk is improper. Accordingly, reversal of the rejection of claims 1, 3, 5, 9-15, 17, 20-28 and 32 is respectfully requested.

2. Claim 2

Claim 2 recites that the first device comprises a firewall filter. The Final Office Action states that Goldstone discloses this feature and points to paragraph 42, lines 1-12 for support (Final Office Action – page 5). Goldstone at paragraph 42 may disclose using a firewall to detect

an attack. Goldstone, however, does not disclose that the firewall filter is able to forward attack information using a link state routing protocol or a path vector routing protocol, as required by claim 2. Fedyk, as discussed above, discloses that routers may use a link state routing protocol to communicate routing information. Fedyk, however, does not disclose that a firewall filter may use such a protocol. Further, as discussed in Appellant's specification at, for example, paragraph 80, conventional firewalls, such as the firewall in Goldstone, are not equipped to handle routing protocols. Therefore, even if routing protocols are known, it is not conventional or obvious for a firewall filter to communicate using either a link state routing protocol or a path vector routing protocol, as required by claim 2.

For at least these reasons, Appellant respectfully submits that the rejection of claim 2 under 35 U.S.C. § 103 based on the combination of Goldstone and Fedyk is improper. Accordingly, reversal of the rejection of claim 2 is respectfully requested.

3. Claims 4, 18 and 29

Claim 4 recites that the first device comprises a packet generating element configured to generate a link state routing packet that includes the attack information. As discussed above, the combination of Goldstone and Fedyk does not disclose or suggest the use of a link state routing protocol or a path vector routing protocol for forwarding attack information. Therefore, the combination cannot further disclose or suggest a packet generating element configured to generate a link state routing packet that includes the attack information, as required by claim 4.

For at least these reasons, Appellant respectfully submits that the rejection of claim 4 under 35 U.S.C. § 103 based on the combination of Goldstone and Fedyk is improper.

Accordingly, reversal of the rejection of claims 4, 18 and 29 is respectfully requested.

4. Claim 6

Claim 6 recites that the first device forwards the attack information using a path vector routing packet. As discussed above, the combination of Goldstone and Fedyk does not disclose or suggest the use of a path link state routing protocol or a path vector routing protocol for forwarding attack information. Therefore, the combination cannot disclose or suggest forwarding the attack information using a path vector routing packet, as required by claim 6.

For at least these reasons, Appellant respectfully submits that the rejection of claim 6 under 35 U.S.C. § 103 based on the combination of Goldstone and Fedyk is improper. Accordingly, reversal of the rejection of claim 6 is respectfully requested.

5. Claims 33-38, 41-43, 45-48, 50 and 51

Claim 33 recites a method of detecting an attack that includes monitoring incoming traffic at a first device to detect an attack and generating attack information defining characteristics of the attack. Claim 33 also recites transmitting the attack information to a second device via a network using a link state routing protocol, a path vector routing protocol, a markup language protocol or a hypertext protocol.

Similar to the discussion above with respect to claim 1, neither Goldstone nor Fedyk discloses or suggest using a link state routing protocol or a path vector routing protocol to transmit attack information. In addition, neither of these references discloses or suggests using a markup language protocol or a hypertext protocol to transmit attack information.

Therefore, as a factual matter, the combination of Goldstone and Fedyk does not disclose or suggest each of the features of claim 33.

In addition, even if, for the sake of argument, the combination of Goldstone and Fedyk could be fairly construed to disclose or suggest all the features of claim 33, Appellant respectfully submits that the alleged motivation to combine these references does not meet the requirements of 35 U.S.C. § 103 for the reasons stated above with respect to claim 1.

For at least these reasons, Appellant respectfully submits that the rejection of claim 33 under 35 U.S.C. § 103 based on the combination of Goldstone and Fedyk is improper. Accordingly, reversal of the rejection of claims 33-38, 41-43, 45-48, 50 and 51 is respectfully requested.

6. Claim 40

Claim 40 recites that the transmitting includes sending the attack information using a link state routing protocol. Similar to the discussion above with respect to claim 4, the combination of Goldstone and Fedyk does not disclose or suggest this feature.

For at least these reasons, Appellant respectfully submits that the rejection of claim 40 under 35 U.S.C. § 103 based on the combination of Goldstone and Fedyk is improper. Accordingly, reversal of the rejection of claim 40 is respectfully requested.

C. Rejection under 35 U.S.C. § 103 based on Goldstone, Fedyk and Nguyen

1. Claims 19, 30, 31 and 49

As to claim 19, the Final Office Action states that Nguyen discloses an improved method of communication between routers using tunneling which prevents unauthorized access (Final Office Action – page 14). The Final Office Action further states that it would have been obvious to use the encryption approach of Nguyen (apparently inadvertently identified in the Final Office Action as Khosravi) "to insure that the information that is being transmitted to recovery from an attack is from an authorized source and not the attacker" (Final Office Action – page 14). Appellant respectfully submits that the alleged motivation to combine these three references does not meet the requirements of 35 U.S.C. § 103.

For example, the alleged motivation is merely a conclusory statement providing an alleged benefit of the combination. No portion of any of the references is pointed to as providing objective motivation for the combination. Such motivation does not satisfy the requirements of 35 U.S.C. § 103.

Appellant further asserts that Goldstone is directed to preventing a denial of service of attack in a network (Goldstone – Abstract). Fedyk, in contrast, is directed to managing message traffic in a link state routing network (Fedyk – col. 1, lines 8-11). Nguyen, in contrast to both Goldstone and Fedyk, is directed to secure network communications (Nguyen – page 1, paragraphs 0003-0004). These three references are unrelated, other than the fact that each of the references may involve network communications. Appellant asserts that one of ordinary skill in the art would not have looked to combine features from the three references due to the disparate nature of the references. That is, the mere fact that each of the references may involve network

communications does not mean that it would have been obvious to combine features from the clearly disparate disclosures.

Further, the mere fact that one reference allegedly provides some missing disclosure with respect to a claim does not satisfy the requirements of 35 U.S.C. § 103 as to why it would have been obvious to combine the references. For at least these reasons, Appellant asserts that it would not have been obvious to combine the three references without the benefit of Appellant's disclosure.

For at least these reasons, Appellant respectfully submits that the rejection of claim 19 under 35 U.S.C. § 103 based on the combination of Goldstone, Fedyk and Nguyen is improper. Accordingly, reversal of the rejection of claims 19, 30, 31 and 49 is respectfully requested.

VIII. CONCLUSION

In view of the foregoing arguments, Appellant respectfully solicits the Honorable Board to reverse the Examiner's rejections of claims 1-6, 9-15, 17-38, 40-43, 45-51, 61, 62 and 64.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1070 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY SNYDER, L.L.P.

By: /Glenn Snyder/
Glenn Snyder
Reg. No. 41,428

Date: November 27, 2006

11350 Random Hills Road
Suite 600
Fairfax, VA 22030
Telephone: (571) 432-0800
Facsimile: (571) 432-0808

IX. APPENDIX

1. A system for detecting and responding to an attack, comprising:

a first device attached to a network and configured to:

detect an attack based on received traffic,

create attack information, and

forward the attack information to the network using a link state routing protocol or a path vector routing protocol; and

a second device configured to receive the attack information and detect particular traffic based on the attack information.

2. The system of claim 1, wherein the first device comprises a firewall filter.

3. The system of claim 1, wherein the first device comprises:

a filter device configured to perform stateful filtering.

4. The system of claim 1, wherein the first device comprises:

a packet generating element configured to generate a link state routing packet that includes the attack information.

5. The system of claim 1, wherein the second device comprises a router.

6. The system of claim 1, wherein the first device forwards the attack information using a path vector routing packet.

9. The system of claim 1, wherein the second device forwards the attack information to other devices.

10. The system of claim 1, wherein the second device configures a filter based on the attack information.

11. The system of claim 1, wherein the second device uses the attack information for a predetermined amount of time.

12. The system of claim 1, wherein the second device rate limits the particular traffic.

13. The system of claim 1, wherein the second device counts the particular traffic.

14. A method of detecting and responding to an attack, comprising:

detecting an attack at a first device based on incoming traffic;

generating attack information defining characteristics of the attack;

sending the attack information to a second device in a network using at least one of a link state routing packet or a path vector routing packet; and

detecting traffic at the second device based on the attack information.

15. The method of claim 14, including:

configuring the first device to detect traffic based on the detected attack.

17. The method of claim 14, wherein the sending includes:

sending the attack information using a distributed routing protocol.

18. The method of claim 14, wherein the sending includes:

sending the attack information using a link state routing protocol.

19. The method of claim 14, further including:

authenticating the attack information at the second device.

20. The method of claim 14, further including:

sending the attack information from the second device to another device.

21. The method of claim 14, further including:

monitoring the attack at the second device.

22. The method of claim 14, further including:

detecting traffic based on the attack information for a particular period of time.

23. The method of claim 14, further including:

rate limiting traffic that matches attack characteristics defined in the attack information.

24. The method of claim 14, wherein the sending includes:

sending the attack information using one of a markup language or hypertext protocol.

25. A device for detecting an attack, comprising:

an attack detection element configured to detect an attack in incoming traffic;

an attack information generator configured to generate attack information defining characteristics of the attack; and

a transmitting element configured to transmit the attack information to a device on a network using at least one of a link state routing protocol or a path vector routing protocol.

26. The device of claim 25, further comprising:

a filter element configured to filter incoming traffic and forward filter information to the attack detection element.

27. The device of claim 26, wherein the attack information generator is further configured to send attack information to the filter element.

28. The device of claim 25, wherein the transmitting element is further configured to transmit the attack information using a distributed routing protocol.

29. The device of claim 25, wherein the transmitting element is configured to transmit the attack information using a link state routing protocol.

30. The device of claim 25, wherein transmitting element is further configured to transmit the attack information using an authentication mechanism.

31. The device of claim 25, wherein the transmitting element is further configured to transmit the attack information using encryption.

32. The device of claim 25, wherein the attack is a denial of service attack.

33. A method of detecting an attack, comprising:

monitoring incoming traffic at a first device to detect an attack;

generating attack information defining characteristics of the attack; and

transmitting the attack information to a second device via a network using a link state routing protocol, a path vector routing protocol, a markup language protocol or a hypertext protocol.

34. The method of claim 33, wherein the attack is a denial of service attack.

35. The method of claim 33, wherein the monitoring includes:

using information from a filter to detect the attack.

36. The method of claim 33, wherein the generating includes:

sending attack information to a filter for configuring the filter based on the attack.

37. The method of claim 33, further including:

performing stateful filtering on incoming traffic.

38. The method of claim 33, wherein the transmitting includes:

sending the attack information in a packet.

40. The method of claim 33, wherein the transmitting includes:

sending the attack information using a link state routing protocol.

41. The method of claim 33, wherein the transmitting includes:

sending the attack information using a markup language protocol or a hypertext protocol.

42. The method of claim 33, wherein the transmitting includes:

sending the attack information in a secure format.

43. A device for responding to an attack, comprising:

a receiver configured to receive attack information from a first device that sent the attack information;

a configuration element configured to configure a second device based on the received attack information; and

a transmitting element for transmitting the attack information to another device using a link state routing protocol, a path vector routing protocol, a markup language protocol or a hypertext protocol.

45. The device of claim 43, wherein the configuration element comprises:

a filter; and

an attack configuration generator.

46. The device of claim 43, wherein the configuration element is further configured to configure the second device based on filter information.

47. The device of claim 43, wherein the configuration element is further configured to unconfigure the second device after a predetermined period of time after configuring based on the attack information.

48. The device of claim 43, wherein the second device comprises a router.

49. The device of claim 43, wherein the configuration element is further configured to authenticate the received attack information.

50. The device of claim 43, wherein the configuration element is further configured to detect particular traffic based on the attack information.

51. The device of claim 43, wherein the configuration element is further configured to monitor traffic and send monitoring results to the first device.

61. A method for responding to an attack, comprising:

receiving attack information at a central management system from a first device via a network;

managing a response to the attack at the central management system;

receiving, at the central management system, additional attack information from other devices via the network; and

communicating, by the central management system, information associated with the additional attack information to the first device.

62. The method of claim 61, wherein the managing includes:

sending the attack information to other devices via a network.

64. The method of claim 61, wherein the managing includes:

collecting information related to the attack information.

X. EVIDENCE APPENDIX

None

XI. RELATED PROCEEDINGS APPENDIX

None